PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 : H04L 9/00	A1	(11) International Publication Number: WO 87/ 05175
		(43) International Publication Date: 27 August 1987 (27.08.87)

(21) International Application Number: PCT/US86/02644

(22) International Filing Date: 4 December 1986 (04.12.86)

(31) Priority Application Number: 832,819

(32) Priority Date: 24 February 1986 (24.02.86)

(33) Priority Country: US

(71)(72) Applicant and Inventor: WEISS, Jeffrey, A. [US/US]; 17 Maureen Drive, Smithfield, RI 02917 (US).

(74) Agent: KUDIRKA, Paul, E.,; Wolf, Greenfield & Sacks, 201 Devonshire Street, Boston, MA 02110 (US).

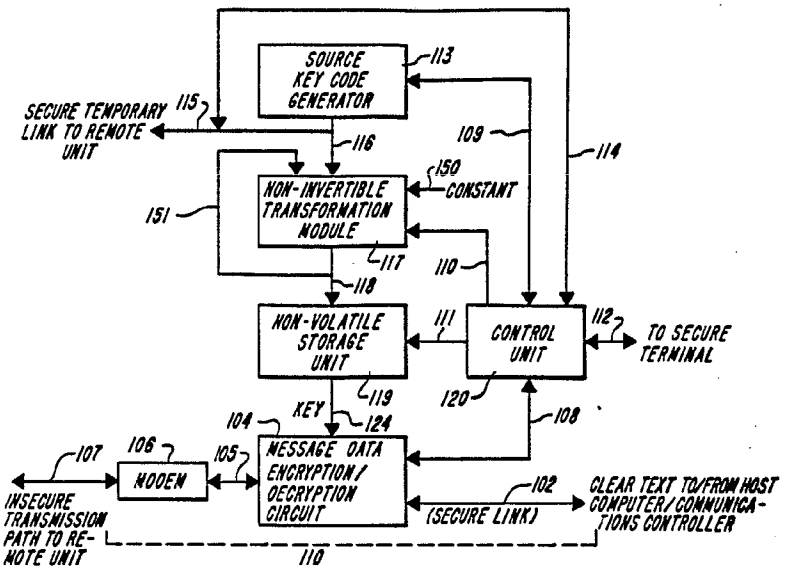
(81) Designated States: AT (European patent), AU, BE (European patent), CH (European patent), DE (European patent), FR (European patent), GB (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR DISTRIBUTING AND PROTECTING ENCRYPTION KEY CODES

(57) Abstract

A method and apparatus for protecting encryption key codes from disclosure and improper usage. To initialize the encryption system, a source number is randomly-generated at a master unit and passed over secure transmission link to a slave unit. Both the master and slave unit perform a non-invertible transformation on the source number to generate two identical master code keys which are then stored in non-volatile memories in both the central site and the slave unit. The source number in each unit is then erased or destroyed. Subsequently, during an information transfer session between the master unit and the slave unit which takes place over an insecure transmission link, the stored master key is used to authenticate the slave unit and may be used to securely transfer additional encrypting keys. Various mechanical methods are used to make the slave unit secure so that it is difficult to extract the master key information from the unit without causing obvious physical damage to the unit. Even if the master key code is extracted, it cannot be loaded into an undamaged unit due to the non-invertible transformation circuitry in that unit; the original source number is required, but is no longer available or derivable. Additional embodiments disclose modifications to conventional key-loader apparatus using the non-invertible transform technique to protect key codes stored in the key-loader from disclosure or improper usage. Apparatus is also disclosed which uses either a non-invertible transform or a cryptographic technique to authenticate key-loader apparatus from a central location.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**FR**	France	**ML**	Mali
AU	Australia	**GA**	Gabon	**MR**	Mauritania
BB	Barbados	**GB**	United Kingdom	**MW**	Malawi
BE	Belgium	**HU**	Hungary	**NL**	Netherlands
BG	Bulgaria	**IT**	Italy	**NO**	Norway
BJ	Benin	**JP**	Japan	**RO**	Romania
BR	Brazil	**KP**	Democratic P. .ple's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SN**	Senegal
CH	Switzerland	**LI**	Liechtenstein	**SU**	Soviet Union
CM	Cameroon	**LK**	Sri Lanka	**TD**	Chad
DE	Germany, Federal Republic of	**LU**	Luxembourg	**TG**	Togo
DK	Denmark	**MC**	Monaco	**US**	United States of America
FI	Finland	**MG**	Madagascar		

METHOD AND APPARATUS FOR DISTRIBUTING AND PROTECTING ENCRYPTION KEY CODES

This invention relates to methods and apparatus for distributing encryption key codes from a central data site to remote access units and for enhancing the security of key codes stored in remote access units.

Due to the proliferation of micro-computers, distributed processing systems have become commonplace. In such a system the data processing functions are spread over a number of separate data processing machines. Each of the machines performs part of the overall processing task and data and results are passed between the machines by means of data links. In many environments, a distributed processing system poses a problem for data integrity and security because sensitive data must be transmitted between the separate data processing machines over transmission facilities, such as telephone lines, which are far from secure. In other cases, a centralized data processing facility may have the capability of being accessed from many

outlying locations by means of data terminals over dedicated data lines or public telephone lines.

Such systems are prone to to misuse from a variety of sources such as illicit access to the system by computer "hackers" or disgruntled employees and improper disclosure or modification of stored information by unscrupulous competitors.

To avoid these misuse problems, cryptographic techniques are becoming more frequently utilized by commercial organizations. These systems modify a message to produce another message which is unintelligible except to those persons possessing proper decoding equipment. In particular, most encryption systems use mathematical algorithms to convert between ordinary messages called "plain text" and encoded messages called "cipher text". The encoding or encrypting algorithm used to convert the plain text into a cipher text is chosen such that it is possible to retrieve the plain text when given the cipher text. To change the cipher text back into the plain text a decoding or decrypting algorithm is used which may be the same or different from the encoding algorithm.

Since many users want to encode not only one message but many and since the intended recipients of the messages are frequently different, a new

encoding algorithm cannot be used for each message or for each of the recipients as this would quickly become highly impractical. Consequently, in practical encryption systems, one encoding algorithm is used with many different parameters, called "keys", instead of many different algorithms. Thus, the key becomes another input, or argument, to the encoding algorithm along with the plain text message characters. In such systems, a decoding key is often required as an additional input to the decoding algorithm with the cipher text in order to be able to reproduce the plain text.

In the more complicated encryption systems, the encoding algorithms are publicly known but the encoded message cannot be recovered from the cipher text without knowledge of the decoding key. Thus, such cryptographic systems are attractive because they do not require that the entire system be kept secure, only the encoding and decoding keys.

However, there exist problems with ensuring security of the encoding and decoding keys if the keys must be distributed from a central site to a plurality of remote units. If the central site and remote units are geographically closely located, then transfer of key information is simple, but in a typical large system where a central data site is accessed by many remote terminals which are

geographically widely separated, then distribution of key codes to the remote sites in a secure manner is often prohibitively expensive. Further, in many prior art data processing systems the keys used for all remote units were identical and thus the loss or theft of a single remote unit required all of the keys to be changed.

Typically, to prevent the key codes from being compromised and to enhance security of the system, master and session keys are used. A master key code is distributed from the central site and is used only to authenticate the user and to encrypt additional encryption keys. After the user is authenticated, the central site then sends an encrypted session key over the insecure data line to the remote site. The session key is used to encrypt the actual data only for that session and is then discarded. Therefore, even if illicit access is gained to the session key, it can only be used for one session.

The master and session key arrangement reduces the probability of illicit access to the master key since the master key is used only briefly, but distribution of master keys remains a problem. One typical method of distributing keys is to generate the master keys at the central site and distribute them to the remote sites in plain text by trusted

couriers. This method is slow, costly and subject to compromise if one or more of the trusted couriers should not have been trusted. In addition, this method is subject to error because the user must enter the key code information into his apparatus and may incorrectly enter the information with the result that he is improperly denied access.

To circumvent this latter problem, "key-loaders" have been developed. A key-loader is an electronic circuit which is programmed with the key information at the central site and then carried by a trusted courier to the remote locations. At each remote location, the key-loader is connected to the remote unit. The key-loader checks an internal identification code in the unit and then automatically loads the correct key information into the unit. While obviating user errors, the key-loader scheme suffers from the remaining problems of manual key distribution in that the courier may inadvertently or intentionally disclose the information or the key-loader may be stolen, the information extracted and then the key-loader returned so that the code theft is not detected.

Several prior art systems rely on mechanical steps to make it difficult to gain internal access to the key-loader to extract the key information from a key-loader without causing obvious,

non-repairable physical damage to the unit. However, in most cases, such access can still be gained with far less sophisticated resources and expense than the resources and expense required for the successful crypto-analysis of the encoded data and underlying keys. This is especially true when the key loaders and remote units are mass-produced and it is possible to purchase duplicate units on the open market. For example, one simple method which could be used to obtain unauthorized access to the key information would be to steal a key-loader, obtain, through mechanical or electronic means, the key code (physically destroying the key-loader, if necessary) and then enter the code into a duplicate, undamaged key-loader unit which is then replaced to hide the theft.

Another prior art approach for securing key information in a key-loader is to encrypt the keys by using another password as an encryption key prior to their insertion into the key-loader. The password may be known to the courier who carries the key-loader from site to site, or transported independently to the remote site. Obviously, with such a system, if the password can be intercepted or otherwise obtained prior to, following, or during its entry into the remote unit, then any keys copied from the key-loader can also be decrypted.

Even if the key information is safely distributed, there remains the problem of keeping the information secure, since, in many cases, remote units are located in offices or other insecure locations to which illicit access can easily be gained during off-work hours. Although, again it is possible to make it difficult to extract key information from a data access unit by various mechanical means, it would still be possible to steal the unit, extract the key code, enter the code into a duplicate, undamaged unit and then replace the unit to hide the theft.

Most prior art security techniques relating to the extraction and reloading of key codes stored in vulnerable remote site units have relied upon mechanical, electrical or password safeguards to prevent access to the stored key code, but such practices fall short of masking the key code itself so that theft of the code will not significantly impair the security of the system.

Accordingly, it is an object of this invention to provide means for distributing and storing a key code which renders undetected theft of the key code highly unlikely.

It is another object of the invention is to provide a remote unit or key-loader device which cannot be loaded with a known key code even in the

event that the master key code and master key code encoding algorithm are learned by an unauthorized user.

It is a further object of this invention to provide a remote unit or key-loader device which is compatible with standard encoding/decoding techniques but has improved security.

The foregoing problems are solved and the foregoing objects are achieved in accordance with illustrative embodiments of the invention in which the encoding and decoding key codes stored at the central site and the remote unit are generated from a common source number which is not stored in either location. The code generation circuitry is such that the key codes cannot be regenerated unless the original source number is known. Therefore, even if the remote unit is stolen and the code extracted, the key code cannot be reloaded into an undamaged unit, because the original source number is not stored in the unit and cannot be determined from the key code. Mechanical means are provided for preventing tampering of the unit without causing non-repairable physical damage so that any attempt to illicitly obtain the key codes or to load key codes directly into the unit other than through the code generation circuitry will result in observable

damage.

More particularly, to initialize the system, a secure data line is used to apply a source number, which may be a random number or a number chosen by the user, from the central site unit to the remote site unit. Both units generate a master key code by passing the source number through circuitry which performs a non-invertible transformation on the source number. A non-invertible transformation is an encoding technique which produces an output number from which the input number cannot be determined even if both the output number and the non-invertible transform algorithm are known. The source number is then destroyed or deleted from both units.

Consequently, in the event an unauthorized user succeeds in gaining access to the master key code and the key code encoding algorithm, such user will not, in any practical manner be able to generate or predict the source number. Since the key code can only be loaded into the remote unit through the transform circuitry, the thief will not be able to regenerate the master key code in a duplicate remote unit without also destroying that unit.

The key code thus loaded into the remote unit is used as a master key to authenticate the unit and to load other encryption keys into the unit, however,

none of these latter keys replace the master key which must be loaded via the central site through the non-invertible transform.

Figure 1 is a block schematic diagram of a portion of the central site apparatus used for generating key code information and encrypting and decrypting messages.

Figure 2 is a block schematic diagram of a portion of the remote data unit used for receiving and storing key code information and encrypting and decrypting messages.

Figure 3 is a block schematic diagram of a conventional D.E.S. encryption circuit used as a circuit for performing non-invertible transforms.

Figure 4 is a block schematic diagram of a portion of key-loader apparatus which may be used to manually deliver key codes to remote sites.

With reference to Figure 1, typical central site apparatus 110 includes data encoding/decoding unit 104, key code generating and storage units 113, 117 and 119, control unit 120 and modem 106. Data encoding circuitry 104 may comprise any of a variety of well-known encoding/decoding circuits which use key codes to encrypt or decrypt data. With such systems, plain text data generated by a host

computer system is transmitted over secure message data lines 102 to the input of data encryption/decryption module 104.

Data encryption/decryption module 104 can embody one of any number of well-known techniques of data encryption. The most popular method of encryption presently used in the United States is the known as the "data encryption standard" or D.E.S. The theory of operation and practical circuits using this encryption method are well-known and discussed in detail in Federal Information Processing Standard (FIPS) Publication No. 46 and U.S. Patent 3,958,081. The basic algorithm set forth in the foregoing D.E.S. publications (the D.E.S. algorithm) uses a digital key code consisting of 56 binary bits, and performs a non-linear decoding or encoding of plain text data in blocks of 64 bits to produce cipher text. Federal Information Processing Standard No. 81 shows several feedback configurations which enable data to be encrypted in blocks of 1 to 64 bits. Illustratively, data encryption module 104 may be a D.E.S. encryption/decryption circuit and may be implemented by a special purpose hardware circuit or may be implemented by means of a suitably-programmed microprocessor.

The 56-bit digital key codes used by module 104

to encrypt and decrypt data are stored in non-volatile storage unit 119. Since unit 110 is a central site unit, many key codes may be stored in storage unit 119. Accordingly, storage unit 119 may illustratively be a magnetic disk unit or other non-volatile storage medium. As will be hereinafter discussed in detail, after control unit 120 authenticates a remote site, it provides address signals over bus 111 to storage unit 119 to cause it to produce the corresponding key code (or codes, if the encryption code and decryption code are not the same) which are then sent, via bus 124, to encryption/decryption module 104. In response to the key code on bus 124 and plain text data on bus 102, encryption/decryption module 104 generates cipher text and applies it to bus 105. Bus 105, in turn, applies the cipher text data to modem 106. Control unit 120 controls authentication, key loading and encryption/decryption operations in encoder/decoder unit 104 via control signals 108.

Modem 106 serves as a modulator to transform digital cipher text data into signals which can be transmitted over various types of data transmission media such as dial telephone lines, dedicated data lines or other transmission media to the various remote sites (not shown in Figure 1). The design and construction of data encryption module 104 and

modem 106 are well-known to individuals skilled in the communication arts and form no part of the present invention. Accordingly, neither circuit will be discussed in detail hereinafter.

Similarly, cipher text generated by the remote sites and sent to central site unit 110 arrives over data lines 107 and is demodulated by modem 106 to produce digital cipher data on line 105. The digital cipher data is provided to encryption/decryption circuit 104 which then generates plain text that is provided to the host computer system via link 102.

In addition to storage unit 119, the key distribution and management portion of central site 110 comprises a source number generator 113, a non-invertible transform module 117 and an encryption and key control unit 120. These pieces of apparatus function as described in detail to generate and distribute keys in a secure manner in accordance with the invention.

As shown in Figure 2, remote site unit 200 comprises encrypting/decrypting unit 241, key handling units 232 and 246, control unit 248 and modem 238. Data lines 207, which may be secure or unsecure, connect modem 238 to the central site and transmit or receive the cipher text carried thereon to modem 238. Modem 238, in turn, demodulates

signals transmitted on lines 207 to produce digital cipher text data on lines 270. Alternatively, modem 238 receives digital cipher data on lines 270 and converts the data into signals for transmission on lines 207.

Data output 270 of modem 238 applies digital cipher text data to data encryption/decryption circuit 241. As with the encryption/decryption circuit 104 of the central site unit, encryption/decryption circuit 241 receives one or more encoding/decoding keys from non-volatile storage unit 246 via bus 272. Since the remote site unit need only store the code keys pertaining to itself, storage unit 246 may comprise an electrically erasable programmable read-only memory (EEPROM) or other small, non-volatile storage area which is not erased when power is removed from the unit.

In response to the code key provided over bus 272 to encryption/decryption circuit 241, the decryption portion of encryption/decryption circuit 241 decrypts the cipher text data in accordance with its internal decryption algorithm and the key code to regenerate the plain text data transmitted from the central site unit 110 (Figure 1). Circuit 241 applies the plain text data to secure lines 243 for transmission to the local user.

Outgoing plain text data presented to the unit on lines 243 by the local user is, in turn, encrypted by the encryption portion of circuit 241 and sent as cipher text, via lines 270, to modem 238 for transmission over lines 207.

In addition to storage unit 246, the key management section of remote unit 200 comprises non-invertible transformation module 232 and control unit 248 which operate in conjunction with their counterparts in the central site to generate and manage the key code information.

As previously mentioned, the inventive system uses a combination of master and session keys to provide increased security during operation. The first step in the initialization of the system or in the addition of new remote units to the system is the generation and distribution of master key code information for each remote unit which is added to the system. To insert master key information into a remote unit, the unit is connected by means of data links 215 and 115 to the central site. Data links 115 and 215 must be secure and not subject to line taps. Typically, the remote unit will be brought to the physical location of the central site for master key generation (alternatively, a secure key-loader, discussed below, may be employed). Although bringing the remote unit to the central location may

present some difficulty if the remote site is not geographically close to the central site, in accordance with the invention, the master key data is more secure than with prior art arrangements and thus, it is presumed that the master key generation routine will not have to be repeated often.

To generate the master key code, a central site security officer instructs control unit 120, via secure communications path 112, to generate and store a master key. In response to the security officer's instructions, control unit 120 instructs source number generator 113, by means of control bus 109, to generate a 56-bit digital number. Source number generator 113 may be any secure source of 56-bit digital numbers such as a protected memory. The number is latched in the output registers of generator 113. However, it is desirable that the source number not be stored after it is used in the generation process to increase the difficulty of re-generating the master key code. Accordingly, in the preferred embodiment, source number generator 113 may comprise a random number generator which will provide source numbers which are sufficiently random such that even the knowledge of one or more prior numbers will not enable an observer to predict, with any significant probability, the values of subsequently generated numbers. A number

of conventional techniques for generating such random numbers exist. Example techniques are described in detail in U.S. Patent Nos. 4,281,286 and 4,313,031. The 56-bit number may have additional bits added for error-checking purposes. In the preferred embodiment of the invention, the source number has eight appended parity checking bits for error detection purposes.

The random source number is transmitted as plain text to non-invertible transform circuit 117 in the central site and, via secure data buses 115 and 215, to non-invertible transform circuit 232 in remote unit 200. Transform circuits 117 and 232 mathematically process the source number to produce a 56-bit master key digital code number. The particular mathematical process chosen is known as a non-invertible transform. As previously mentioned, a non-invertible transformation is a mathematical manipulation which accepts an input number and produces an output number from which the input number cannot be determined even if both the output number and the non-invertible transform algorithm are known. Circuitry which performs such transformations may be embodied by any one of several conventional circuits. In the preferred embodiment of the invention, the non-invertible transformation is conveniently performed by using a

conventional D.E.S. encryption circuit as shown in Figure 3.

In Figure 3, the 56-bit source number 305 is applied to the D.E.S. encryption module 301, via bus 306, as the encryption key. A 64-bit predetermined constant number 304 is applied, via bus 303, to the data input and the least significant 56 bits of the resulting 64-bit output 302 are retained as the master code key number. With this arrangement, the non-invertible characteristics of the resulting transformation depend upon the cryptographic strength of the D.E.S. algorithm relative to protection of the encryption key. Unless a weakness in the algorithm is subsequently discovered, the D.E.S. algorithm has the property that given the input data (in this case the predetermined constant number) and the resulting output (in this case the master key code), the encryption key (the source number) can only be found by an exhaustive search of all possible encryption key numbers - a task which is beyond the capability of present computers.

In the preferred embodiment, both transform circuits 117 and 232 are identical and use the same predetermined constant as a data input. The constant is applied over line 150 to transform module 117. Likewise, the same constant is applied to transform module 232 over line 252 in remote unit

200. Thus, the master key codes produced by both circuits are identical. The master key code output 118 from transform circuit 117 in Figure 1 is applied to non-volatile storage means 119. Further, control unit 120 instructs storage unit 119, via control bus 111, to accept and store the master key code. Control unit 120 may be any of a number of well-known circuits, such as a microprocessor. The master key code is thereupon stored in storage means 119 as the master encryption key which is applied to encryption module 104 to control the data encryption/decryption algorithms as previously described. Control unit 120 may also store a suitable identification number in storage unit 119 which identification number is associated with the master key code so that the proper key code can be used when a remote unit identifies itself upon requesting access to the system.

Similarly, with reference to Figure 2, the source number is applied via lines 215 to transformation module 232 of remote unit 200. The output of transform circuit 232 on lines 280 is applied to non-volatile storage circuit 246. Further, in response to the source number appearing on lines 215, as seen from bus 253, control unit 248 instructs non-volatile storage unit 246, via control bus 250, to store master key information on lines

280, which master key information is to be used for encryption and decryption as previously described.

After loading of the master key information, control unit 120 commands source code number generator 113 to destroy the source number by clearing its output register. Consequently, the source number, in recognizable form, is not resident in either the central unit 110 or the remote unit 200 after the loading of the master key information.

After the master key code information has been entered the data links connecting the central unit and the remote unit are disconnected and the remote unit is returned to its operating location.

Once the master key code has been stored at the remote site, various security measures are taken to ensure that it is not extracted. To this end, non-invertible transform unit 232 and storage unit 246 in remote unit 200 are packaged so that the non-invertible transform module 232 cannot be circumvented and the master key code loaded directly into non-volatile memory 246. For example, storage unit 246 may illustratively be a battery-backed CMOS random access memory and the entire key management portion of remote unit 200 may be fully encapsulated in epoxy. One or more safety mechanisms can be encapsulated with the circuits so that if the unit is chemically or mechanically opened the power

supplied to the CMOS random access memory by the battery circuits will be disconnected and all keys will be lost.

Alternatively, a single integrated circuit chip containing both the transform circuit 232 and the storage unit 246 can be used.

During operation of the remote unit additional safeguards are used to ensure security of the system. For example, access to the remote unit may be restricted to a user having a valid password. The password could be stored in the storage unit 246 in the unit along with the key code information and may be changed at will by a user possessing the password. However, a password so stored would be vulnerable to disclosure were a thief able to gain access to the storage unit as previously described. To prevent disclosure of the password, in the preferred embodiment, the password is not explicitly stored in storage unit 246. Instead, a predetermined fixed value is encrypted by means of an additional D.E.S. encryption circuit utilizing the password as the key code and the encrypted value is stored in the unit's memory.

When a user desires to use the remote unit, he enters his password and it is used as a key code to decode the encrypted value. The decoded value is compared to a copy of the value stored in the

storage unit 246. Only if the values match is the password is considered valid. As added precautions, the central site may periodically require password changes and, if after a predetermined number of trials, the proper password is not entered into the remote unit, the unit may be programmed to erase all the internally-stored key information rendering the unit useless until reactivated by a central site.

In addition, to further increase the difficulty in using illicitly-obtained master key code information in the event that the physical safeguards discussed above be successfully circumvented, the master key information can also be encrypted by using a D.E.S. encoding module with the user's password as the key code . Thus, when the user enters his password it is used to decrypt the stored key code as well as the stored predetermined value (as mentioned above) for usage during a particular session. Accordingly, even if a remote unit is stolen, it is worthless without knowledge of the rightful owner's password.

However, in accordance with the invention, even if the encryption module is successfully violated and the key codes extracted and the owner's password is known, because of the non-invertible transform which is used to load the master key information as described above, the extracted key information

cannot be inserted into the memory of an undamaged unit through the normal transfer lines 215. In order to insert the master key into the undamaged unit the thief would have to know the original source number which was passed through the non-invertible transform to generate the key code. Since this number was destroyed after the initial loading of the master key information, it is impossible for the thief to obtain knowledge of it. Further, due to the packaging techniques as described above, the key code information cannot be directly loaded into the remote unit storage module.

For further security, the transfer of information between the remote unit and the central site over links 107 and 207 may be accomplished by the use of the multiple key codes. Such multi-level key hierarchies are well-known in the art. Illustrative systems are disclosed in U.S. Patent nos. 4,238,853 and 4,386,234. An additional document, ANSI Standard X9.17, describes and defines the characteristics of a key management system using two level and three level key hierarchies.

Illustratively, three key levels are used. The first key code is the master key code which, as previously discussed, is loaded at the central site. This code is used at the start of each data session for authentication of the remote unit as

described below.

The second key is a primary encryption key which is used to encrypt each session key and another primary key to transfer these keys from the central site to the remote location. Each primary encryption key is used once then destroyed.

The final key used in the transfer is a session key. This key is used to encrypt and decrypt data which passes between the central site and the remote unit. The session key is used for one data session and is then destroyed. With the three above keys, the initiation of communications between a central site and a remote unit proceeds as follows:

To initiate communications with a central site, a user at the remote unit must manually supply a valid password to the unit. After the password is supplied, the remainder of the initialization sequence is performed automatically by the remote unit circuitry without user control.

More specifically, after receiving the user password, the unit uses it to decrypt the primary encryption key, master key and the predetermined constant which as discussed above have already been stored in the unit's internal memory. If the value obtained by decrypting the stored predetermined constant matches a predetermined value stored in the unit, the password is declared valid and the remote

unit initiates a data connection between itself and the central site.

After the data connection is established, an authentication routine is initiated. Specifically, the central site unit transmits in plain text a message identifying itself and requesting the remote unit's identification number corresponding to that central site. The remote unit then uses the central site's identification number to look up its corresponding equipment identification number and encryption keys which are to be used for communications with that central site. The remote unit then returns its identification number to the central site in plain text.

Upon receiving the remote identification number, the central site uses it to look up the corresponding access limitations (if any) and the corresponding master key code in non-volatile storage unit 119. If the remote unit is currently authorized to access the site, the central site generates a random number using generator 113 and encrypts the number using the remote unit's master key code as the key. The resulting encrypted cipher text is then returned to the remote unit.

The remote unit decodes the cipher text by using its internally-stored copy of its master key code to obtain the random number, increments the number,

re-encrypts the result in its master key code and sends the resulting cipher text back to the central site.

At the central site, the central site decrypting equipment decrypts the returning cipher text and compares it to the original random number sent to the remote unit. If the returning text corresponds to the incremented random number, the remote unit is considered as authenticated.

The central site next transfers a session key and a new primary encryption key to the remote site. More specifically, the central site searches in memory 119 for the active primary encryption key code for that remote unit. When the primary key is obtained, a session key for use in the current session and a new primary key for use in re-establishing communications during the next data session are generated in unit 113, saved in unit 119, encrypted using the current active primary encryption key code and sent to the remote unit. After reception has been acknowledged, the current primary key is erased from central site memory 119. Thus, the primary key is used only once as a "transport vehicle" for the session and for the new primary key before it is replaced with a new random key.

This changing or evolution of the primary key

for each new data session provides an additional layer of security which enables the detection of a duplicate remote unit which attempts central site access using stolen keys.

The principles of the instant invention can also be extended to increase the security of electronic key loaders. As previously mentioned, key loaders are electronic devices which can be loaded with master key information at a central site and carried to various remote sites where, in response to an identification code generated by a remote unit, the key loader unit can electronically transfer appropriate key code information to the unit.

The problem with such key loaders is that they must be physically carried between sites by a courier and, if the courier is not trustworthy, then the entire security system can be compromised. Even if the courier is trustworthy, the key loader can be stolen and the key information extracted by means of suitable electronic equipment which generates identification codes. The extracted key information can be stored and then the key loader can be returned unharmed so that the theft of the information will not be detected.

In order to combat this latter problem, some key loaders have been designed so that the key information can only be extracted once. After key

information has been removed, it is internally destroyed and then the key loader must be reprogrammed at the central site. With this latter type of unit, the empty key loader cannot be returned unchanged to hide the theft. However, even this type of unit can be easily circumvented by extracting the key information (damaging or destroying the unit, if necessary), storing the key information and then reloading the stored information into the original (if undamaged) key loader, or an undamaged duplicate key loader purchased on the open market.

The invertible transform arrangement of the instant invention can be used with the latter type of key loader to increase security by preventing the key information from being reloaded into an undamaged unit. In particular, in accordance with the present invention, the key loader and the central site are equipped with non-invertible transform circuits in a manner similar to the remote unit discussed in detail above.

With reference to Figure 4, a typical key loader apparatus 400 constructed in accordance with the present invention includes, along with other circuitry (not shown), data encoding unit 404, non-volatile storage unit 403, non-invertible transformation unit 402, and control unit 401.

Control unit 401 may be comprised of any well-known sequencing circuitry such as hard-wired logic or a microprocessor.

Non-invertible transformation module 402 is identical in construction and function to non-invertible transform units 117 and 232 shown in Figures 1 and 2, respectively, and discussed above. Non-volatile storage unit 403 is identical in construction and function to storage unit 246 shown in Figure 2. Similarly, encryption/decryption circuit 404 is identical in construction and function to units 104 and 241 (Figures 1 and 2, respectively). Non-invertible transformation module 402 and encryption/decryption circuit 404 may be constructed from discrete logic circuitry or integrated circuit chips, or may be implemented as software programs which execute in the control unit 401.

In accordance with one aspect of the invention, non-invertible transformation unit 402, encryption/decryption unit 404 and storage unit 403 are physically packaged together such that key codes cannot be loaded directly into non-volatile memory 403 without passing the codes through non-invertible transform unit 402. Furthermore, the construction is such that key codes loaded into encryption/decryption unit 404 can not be externally

observed. These latter results can be achieved in a number of well-known ways. For example, unit 400 may be fully encapsulated in epoxy plastic along with special circuits that can detect penetration into the epoxy and, in the event of such penetration, destroy or erase key information stored in storage unit 403. Alternatively, the storage, transform and encryption functions may be constructed on a single-chip integrated circuit.

Key loader unit 400 is initialized by bringing it to a secure central site such as that shown in Figure 1. During such initialization, source code generator 113 at the central site generates two random numbers. One random number is used to generate the key code for each remote unit and must be generated separately for each unit. The other random number (as will be described in detail below) is used to authenticate the key loader and may be the same (or different) for each remote unit which is to be loaded from the key loader apparatus. One of these random numbers (designated as random number 1) is passed through non-invertible transformation module 117 once, and stored in central site non-volatile memory 119 along with a code identifying the remote unit associated with the number. This first transformed random number is used, as will be hereinafter described, during an

authentication procedure for authenticating the key loader unit used to transfer key information from the central site to the remote unit. The remaining random number (designated as random number 2) is passed through non-invertible transform circuit 117 and then the transformed result is again passed through non-invertible transform circuit 117 via link 151. The result of two passes through the non-invertible transform circuit is subsequently stored in storage unit 119 as the master key for the corresponding remote unit.

Both of the random source numbers generated by the central site are also provided to key loader 400 via secure data links 115 and 408. The number pair are sequentially passed, via link 405, to non-invertible transform module 402. The transformed results are passed, via link 409, to non-volatile storage unit 403, where both transformed numbers are stored under the control of control unit 401 by means of control bus 406. In addition, an identification number uniquely identifying the remote unit to the central site is stored in unit 403 with the transformed number pair. The random numbers used in the initialization are then destroyed or erased from both the key loader circuitry and the central site. The above process is repeated for each remote unit to which

key information is to be transferred.

To transfer master key information to a remote site (which, illustratively, contains circuitry in accordance with the invention as described above) the key loader is physically carried to the remote unit, where a secure connection is established between the remote unit and the key loader via links 408 and 215. The key loader control unit 401 then forwards a request to the remote unit control circuit 248 for an identification number for that remote site. The identification number is supplied by remote site control unit 248 to key loader controller 401, which thereupon checks storage unit 403 for the identification number to locate the corresponding stored number pair. The value stored in storage unit 403 corresponding to the transformed value of random source number 2 is forwarded to the remote unit as the new master code encryption/decryption key. More particularly, transformed random number 2 is read from memory 403 and transferred to control unit 401 via link 410.

The transformed number is transferred via links 408 and 215 to the remote unit where it is then passed through non-invertible transformation module 232 and the twice-transformed result is stored as the master key code in non-volatile storage unit 246. The stored number is now identical to the

original source random number 2 which was stored in the central site following its passage through non-invertible transformation module 117 twice as previously discussed.

During a subsequent authentication of the remote unit, the stored master key code is used as previously described to authenticate the unit. In accordance with the invention, even if a key loader unit is stolen and the key information extracted, the extracted key information cannot be reloaded into the same key-loader unit, or a similar undamaged unit, because upon loading, the key information is passed through the non-invertible transform unit in the key-loader, and thus the result will not be the master key code information stored in the central site, but instead a transform of the master key code information. In order to install a duplicate of the original master key code information in the key loader, it is necessary to have knowledge of the random source number which, as previously described, is destroyed after the key loader is loaded with key information.

A modified authentication procedure may be performed to insure that the key information stored in the remote unit, was transferred to the remote unit from the key loader that the central site originally loaded, and not from a duplicate key

loader in which the non-invertible transformation has been defeated. More particularly, during the transfer of key information from the key loader to the remote site, an additional operational sequence can be programmed into the devices. During this modified sequence, the remote unit generates a random, or pseudo-random number, in control unit 248, stores the number in storage unit 246 and also passes the number to the key loader module over links 215 and 408. The key loader module control unit 401 forwards the number received from the remote unit to its internal encryption/decryption circuit 404, via link 407.

The number received from the remote unit is encrypted by circuit 404 using, as a key code, the transformed result of original random number 1 retrieved from non-volatile storage unit 403. The encrypted result is returned to the remote unit 200 and stored in non-volatile storage unit 246. Subsequently, when remote unit 200 is attached to central site unit 110, via insecure links 107 and 207, and an authentication procedure is performed, in addition to the information transferred between the central site and the remote unit as described above, the random number generated by the remote unit and the result of the encryption of the random number by the key loader unit (both of which are

stored in unit 246) are passed to the central site unit. At the central site, the random number received from the remote unit is encrypted using the random source number 1 stored in the central site memory during the key loader initialization procedure (described in detail above). The result of this latter encryption is compared to the encrypted result received from the remote unit. A match indicates that the key loader used to load key information into the remote unit was the original key loader.

With this modified procedure, even if a key loader is stolen, the proper identification code is illicitly obtained and presented to the key loader, the associated key is read out, and the thief constructs a new key loader module which does not have a non-invertible transform unit connected between the module input and the storage unit, the transformed result of random source number 1 is still required to complete the previously-described authentication procedure. This latter number can only be obtained through cryptographic analysis of the original key loader by analyzing its response to externally-applied signals (a procedure which is quite difficult) or, alternatively, through physical means (which is also difficult if all key loader functions and non-volatile storage are physically

protected as described above).

It is also possible to use other safeguards to authenticate the key loader using the authentication key technique discussed above without using an invertible transform approach. For example, if the key loader is constructed so that it will only deliver a particular key to a remote unit one time (until reset at the central site) and so that a new authentication number must be loaded into the key loader at any time that new keys are loaded into the key loader, then an authentication number may be directly loaded and stored in the key loader unit without passing the number through a non-invertible transform. This latter authentication number is used during an authentication procedure as previously discussed to authenticate the key loader unit.

More particularly, as previously discussed, the remote unit generates a random, or pseudo-random number, in control unit 248, stores the number in storage unit 246 and also passes the number to the key loader module over links 215 and 408. The key loader module control unit 401 forwards the number received from the remote unit to its internal encryption/decryption circuit 404, via link 407.

The number received from the remote unit is encrypted by circuit 404 using, as a key code, the

stored authentication number retrieved from non-volatile storage unit 403. The encrypted result is returned to the remote unit 200 and stored in non-volatile storage unit 246. Subsequently, when remote unit 200 is attached to central site unit 110, via insecure links 107 and 207, and an authentication procedure is performed, in addition to the information transferred between the central site and the remote unit as described above, the random number generated by the remote unit and the result of the encryption of the random number by the key loader unit (both of which are stored in unit 246) are passed to the central site unit. At the central site, the random number received from the remote unit is encrypted using a copy of the authentication number stored in the central site memory during the key loader initialization procedure. The result of this latter encryption is compared to the encrypted result received from the remote unit. A match indicates that the key loader used to load key information into the remote unit was the original key loader.

Thus, even if a key loader is stolen, the proper identification code is illicitly obtained and presented to the key loader, and the associated key is read out then the key loader cannot be used to load the key into another (the authentic) remote

unit because the key will only be provided by the key loader once. The thief cannot load the extracted key back into the original key loader or a duplicate because this requires knowledge of the original authentication number. This latter number can only be obtained through cryptographic analysis of the original key loader by analyzing its response to externally-applied signals (a procedure which is quite difficult) or, alternatively, through physical means (which is also difficult if all key loader functions and non-volatile storage are physically protected as described above).

Additional procedures may be employed to increase the level of protection offered by the inventive apparatus. For example, a procedure may be followed in which the first time a remote unit is loaded with master key information, it must be physically transported to the central site to have the master key loaded as previously described. If, in the future, the master key information stored in the remote unit is changed by means of a key loader, in addition to transforming the master key information obtained from the key loader as set forth above, the remote unit logically combines (by means of an exclusive-OR function) the transformed information transferred from the key loader with the master key information currently stored in the

remote unit memory.

More specifically, when a new key is to be generated by the central site unit for transfer to the remote unit by key loader, the random source number which is to be used to generate the new master key information is passed through non-invertible transformation module 117 twice as previously described. However, before being stored in memory 119, the twice-transformed result is exclusive OR-ed with the presently-active master key information for the remote unit and the result of the logical combination is stored in unit 119 as the new master key information (the circuitry to perform the exclusive-OR operation may be part of the memory control circuitry in unit 119). The source number is also transferred to the key loader unit where it is transformed and stored.

As previously described in detail, when the master key information is loaded into the remote unit memory from the key-loader, it is transformed again to generate the master key information to be stored. In accordance with the additional protection procedure, the twice-transformed result is also exclusive-ORed with the active master key and is stored as the new master key in storage unit 246.

The new master key information is then used to

authenticate the remote unit during the next information transfer session in a manner previously described. Following a successful authentication and primary key transfer from the central site using the new master key, the previous master key information is deleted or erased from both the central site and remote units. With this additional procedure, if the above-described key loader security is defeated, or a key loader is used to load key information into remote units other than the intended recipients, system security still is not compromised, as knowledge of the remote unit's currently active master key is required to make proper use of the master key information in the key loader.

What is Claimed is:

1. In a data communication system having a first communication unit and a second communication unit, means in each unit for encrypting and decrypting data using key codes, apparatus for generating key codes for storage in said first unit and in said second unit to allow said units to communicate, said apparatus comprising,

means for generating a source number,

a non-invertible transformation means located in said first unit responsive to said source number for generating a master key code,

means for storing said master key code in said first and second units,

means for destroying all copies of said source number in at least said first unit after storage of said master key code, and

means located in said first unit for preventing entry of master key code information into said storage means associated with said first unit except master key code information produced by said first transformation means.

2. In a data communication system, the apparatus according to Claim 1 wherein said source number generator generates a random number.

3. In a data communication system, the apparatus according to Claim 1 wherein said non-invertible transformation means comprises a D.E.S. encryption unit using a predetermined constant for a data input and said source number for a key code input.

4. In a data communication system, the apparatus according to Claim 1 wherein said source number generator comprises means for generating a random number and means for temporarily storing a generated number and said means for destroying said source number comprises means for clearing said source number generator temporary storing means.

5. In a data communication system, the apparatus according to Claim 1 wherein said means for preventing entry of any master key code information into said storage means in said first unit comprises encapsulating material encapsulating both said non-invertible transformation means and said storage means located in said first unit.

6. In a data communication system having a first

communication unit and a second communication unit, means in each unit for encrypting and decrypting data using key codes, said apparatus comprising,

a random number generator for generating a random source number,

a first non-invertible transformation means located in said first unit responsive to said random source number for generating a first master key code,

a second non-invertible transformation means located in said second unit responsive to said random source number for generating a second master key code, said first transformation means being mathematically related to said second transformation means so that said first master key code is identical to said second master key code,

means located in said first unit and responsive to said first master key code for storing said first master key code,

means located in said second unit and responsive to said second master key code for storing said second master key code,

means for destroying copies of said random source number in at least said second unit after storage of both of said master key codes, and

means located in said second unit for preventing entry of any master key code information into said storage means located in said second unit except master key code information produced by said second transformation means.

7. In a data communication system, the apparatus according to Claim 6 wherein said first non-invertible transformation means comprises a D.E.S. encryption unit using a predetermined constant for a data input and said random source number for a key code input.

8. In a data communication system, the apparatus according to Claim 6 wherein said second non-invertible transformation means comprises a D.E.S. encryption unit using a predetermined constant for a data input and said random source number for a key code input.

9. In a data communication system, the apparatus according to Claim 6 wherein said random source number generator comprises means for generating a random number and means for temporarily storing a generated number and said means for destroying said source number comprises means

for clearing said source number generator temporary storing means.

10. In a data communication system, the apparatus according to Claim 6 wherein said means for preventing entry of any master key code information into said storage means comprises encapsulating material encapsulating both said second non-invertible transformation means and said storage means located in said second unit.

11. In a data communication system, the apparatus according to Claim 6 wherein both said second non-invertible transformation means and said storage means located in said second unit are fabricated within the same integrated circuit so that no master key code information can be loaded into said storage means located in said second unit except master key code information produced by said second transformation means.

12. A secure data communication system comprising,

a secure central site,

a non-secure remote communication unit,

means in said central site and said remote unit for encrypting and decrypting data using key codes,

a random number generator located in said central site for generating a random source number,

a first non-invertible transformation means located in said central site and responsive to said random source number for generating a first master key code,

a second non-invertible transformation means located in said remote site and responsive to said random source number for generating a second master key code, said first transformation means being mathematically related to said second transformation means so that said first master key code is identical to said second master key code,

means located in said central site and responsive to said first master key code for storing said first master key code,

means located in said remote unit and responsive to said second master key code for storing said second master key code,

means for destroying all copies of said random source number in at least said remote unit after storage of both of said master key codes, and

means located in said remote unit for preventing entry of any master key code

information into said storage means located in said remote unit except master key code information produced by said second transformation means.

13. In a data communication system, the apparatus according to Claim 12 wherein said first non-invertible transformation means comprises a D.E.S. encryption unit using a predetermined constant for a data input and said random source number for a key code input.

14. In a data communication system, the apparatus according to Claim 12 wherein said second non-invertible transformation means comprises a D.E.S. encryption unit using a predetermined constant for a data input and said random source number for a key code input.

15. In a data communication system, the apparatus according to Claim 12 wherein said random source number generator comprises means for generating a random number and means for temporarily storing a generated number and said means for destroying said source number comprises means for clearing said source number generator temporary storing means.

16. In a data communication system, the apparatus according to Claim 12 wherein said means for preventing entry of any master key code information into said remote unit storage means comprises encapsulating material encapsulating both said second non-invertible transformation means and said storage means located in said remote unit.

17. In a data communication system, the apparatus according to Claim 12 wherein both said second non-invertible transformation means and said storage means located in said remote unit are fabricated within the same integrated circuit so that no master key code information can be loaded into said storage means located in said remote unit except master key code information produced by said second transformation means.

18. In a data communication system having a first communication unit and a second communication unit, and means in each unit for encrypting and decrypting data using key codes, a method for generating master key codes for storage in said first unit and in said second unit to allow said units to communicate, said method comprising the

steps of:

A. generating a source number,

B. generating a first master key code by passing said source number through a non-invertible transformation circuit,

C. storing said master key code in said first unit and said second unit,

D. destroying said all copies of said source number in at least said first unit after storage of said master key codes, and

E. preventing entry of any master key code information into said storage means associated with said first unit except master key code information produced by said first transformation means.

19. A method according to Claim 18 wherein step E further comprises the steps of:

E'. encapsulating both said first non-invertible transformation means and said storage means located in said first unit so that entry of any master key code information into said storage means associated with said first unit except master key code information produced by said transformation circuit is prevented.

20. A method according to Claim 18 wherein step E further comprises the steps of:

E". fabricating both said non-invertible transformation means and said storage means located in said first unit within the same integrated circuit so that no master key code information can be loaded into said storage means located in said first unit except master key code information produced by said transformation circuit.

21. In a data communication system having a central site unit and a remote communication unit, means in each unit for encrypting and decrypting data using key codes and means in each unit for storing key codes, a method for generating master key codes for storage in said central site unit and in said remote unit to allow said units to communicate, said method comprising the steps of:

A. generating a random source number,

B. generating a master key code by using said source number as the key code for a D.E.S encryption circuit and encrypting a predetermined constant to produce a master

key code output,

C. storing said master key code in said central site unit and said remote unit,

D. destroying all copies of said source number in at least said remote unit after storage of said master key codes, and

E. preventing entry of any master key code information into said storage means associated with said remote unit except master key code information produced by said D.E.S. encryption circuit.

22. A method according to Claim 21 wherein step E further comprises the steps of:

E'. encapsulating both said D.E.S. encryption unit and said storage means located in said remote unit so that entry of any master key code information into said storage means associated with said remote unit except master key code information produced by said D.E.S. encryption circuit is prevented.

23. A method according to Claim 21 wherein step E further comprises the steps of:

E". fabricating both said D.E.S. encryption circuit and said storage means located in said remote unit within the same integrated

circuit so that no master key code information can be loaded into said storage means located in said remote unit except master key code information produced by said D.E.S. encryption circuit.

24. In a data communications system having a first communications unit, a second communications unit, means in said first and said second communications units for encrypting and decrypting data using key codes, and a portable electronic key loader unit for manually transferring master key codes between said first unit and said second unit, apparatus for generating and storing master key codes to allow said units to communicate, said apparatus comprising,

a number generator for generating a digital source number,

a non-invertible transformation means located in said key loader unit responsive to said source number for generating a transformed code number which is to be used as a master key code,

non-volatile storage means in said key loader unit for storing said master key code,

means for destroying all copies of said

source number in at least said key loader unit after storage of said master key code, and

means located in said key loader for preventing entry of any master key code information into said storage means associated with said key loader unit except master key code information produced by said transformation means.

25. In a data communications system, apparatus according to Claim 24 further comprising,

a second non-invertible transformation means in said first communication unit responsive to said source number for generating a second transformed code number,

means responsive to said second transformed code number for passing said second transformed code number through said second non-invertible transformation means in said first communication unit to generate a twice-transformed code number,

second non-volatile storage means located in said first communication unit for storing said twice-transformed code number,

secure means for transferring said transformed code number stored in said key loader unit to said second communication unit,

a third non-invertible transformation means

located in said second communications unit responsive to said transformed code number received from said key loader unit for generating a key code, and

third non-volatile storage means located in said second communications unit for storing said key code.

26. In a data communications system, the apparatus according to Claim 24 further comprising,

means for generating a second source number,

means responsive to said second source number for passing said second source number through said non-invertible transformation means in said key loader unit to generate a second transformed code number,

storage means located in said key loader unit for storing said second transformed code number, and

means for destroying all copies of said second source number in at least said key loader unit after generation of said second transformed code number.

27. In a data communications system, the apparatus according to Claim 26 further comprising,

means for generating a third source number,

a cryptographic function generator located in said key loader unit and responsive to said third source number and to said stored second transformed code number for generating a unique cryptographic number from said third source number and said stored second transformed code number,

storage means located in said second communication unit for storing said cryptographic number, and

means operable during a subsequent authentication procedure for transferring said third source number and said cryptographic number to said first communication unit.

28. In a data communications system, the apparatus according to Claim 27 wherein said cryptographic function generator comprises encryption means located in said key loader unit and responsive to said third source number and to said stored second transformed code number for encrypting said third source number using said second transformed code number as a key code to generate said cryptographic number.

29. In a data communications system having a first

communications unit, a second communications unit, means in said first and said second communications units for encrypting and decrypting data using key codes, and a portable electronic key loader unit for manually transferring key codes between said first unit and said second unit, apparatus for authenticating said key loader unit comprising,

a number generator for generating a digital source number,

a non-invertible transformation means located in said key loader unit responsive to said source number for generating a transformed code number,

non-volatile storage means in said key loader unit for storing said transformed code number,

means for destroying all copies of said source number in at least said key loader unit after storage of said transformed code number,

means located in said key loader for preventing entry of any master code number information into said storage means associated with said key loader unit except master key code number information produced by said transformation means,

means for generating a second source number,

a cryptographic function generator located in said key loader unit and responsive to said second source number and to said stored transformed code number for generating a cryptographic number from said second source number and said stored transformed code number,

storage means located in said second communication unit for storing said cryptographic number, and

means operable during a subsequent authentication procedure for transferring said second source number and said cryptographic number to said first communication unit.

30. In a data communications system, the apparatus according to Claim 29 wherein said cryptographic function generator comprises encryption means located in said key loader unit and responsive to said second source number and to said stored transformed code number for encrypting said second source number using said stored transformed code number as a key code to generate said cryptographic number.

31. In a data communications system having a first

communications unit, a second communications unit, means in said first and said second communications units for encrypting and decrypting data using key codes, a portable electronic key loader unit for manually transferring key codes between said first unit and said second unit, and means located in said second unit for generating a key loading signal to allow said key loader to load key information into said second unit, apparatus for authenticating said key loader unit comprising,

means for storing a plurality of key codes in said key loader unit,

means responsive to said key loading signal for providing one of said stored key codes to said second unit, said providing means having means reponsive to the transfer of one of said stored key codes to said second unit for disabling said providing means so that said one of said key codes can only be provided to a single communication unit during one key transfer session,

a number generator for generating an authentication number,

non-volatile storage means in said key loader unit for storing said authentication number,

means responsive to the storing of said authentication number in said key loader unit for preventing said means for storing a plurality of key codes in said key loader unit from storing any further keys in said key loader unit unless a new authentication number is also stored in said key loader unit,

means located in said second communication unit for generating a source number,

a cryptographic function generator located in said key loader unit and responsive to said source number and to said stored authentication number for generating a cryptographic number from said source number and said stored authentication number,

storage means located in said second communication unit for storing said cryptographic number, and

means operable during a subsequent authentication procedure for transferring said source number and said cryptographic number to said first communication unit.

32. In a data communications system, apparatus according to Claim 31 wherein cryptographic function generator comprises encryption means

for encrypting said source number using said stored authentication number as a key code to generate said cryptographic number.

33. In a data communications system, apparatus according to Claim 31 further comprising,

a number generator for generating a second digital source number,

a non-invertible transformation means located in said key loader unit responsive to said second source number for generating a transformed master key code number,

non-volatile storage means in said key loader unit for storing said transformed master key code number,

means for destroying all copies of said second source number in at least said key loader unit after storage of said transformed master key code number, and

means located in said key loader for preventing entry of any master key code number information into said storage means associated with said key loader unit except master key code number information produced by said transformation means.

34. In a data communications system, apparatus

according to Claim 33 further comprising,

a second non-invertible transformation means in said first communication unit responsive to said second source number for generating a second transformed code number,

means responsive to said second transformed code number for passing said second transformed code number through said second non-invertible transformation means in said first communication unit to generate a twice-transformed code number,

second non-volatile storage means located in said first communication unit for storing said twice-transformed code number,

secure means for transferring said transformed master key code number stored in said key loader unit to said second communication unit,

a third non-invertible transformation means located in said second communications unit responsive to said transformed master key code number received from said key loader unit for generating a master key code, and

third non-volatile storage means located in said second communications unit for storing said master key code.

35. In a data communications system having a first

communication unit, a second communication unit, and a portable key loader unit, each of said communication units having means for encrypting and decrypting data using key codes, apparatus for authenticating said key loader unit comprising,

means for generating a plurality of source numbers,

non-invertible transformation means located in said key loader unit responsive to one of said source numbers for generating a transformed code number,

non-volatile storage means in said key loader unit for storing said transformed code number,

means located in said key loader for preventing entry of any master key code number information into said storage means associated with said key loader unit except master key code number information produced by said transformation means,

a cryptographic function generator located in said key loader unit, said cryptographic function generator being responsive to said stored transformed code number and to another of said source numbers for generating a cryptographic number from said other source

number and said stored transformed code number, and

means for transferring said other source number and said cryptographic number to one of said communication units for authenticating said key loader unit.

36. In a data communications system, apparatus according to Claim 35 wherein cryptographic function generator comprises encryption means for encrypting said stored transformed code number using said other source number as a key code to generate said cryptographic number.

37. In a data communications system, the apparatus according to Claim 36 further comprising second non-invertible transformation means located in said one of said communication units and responsive to said source number for generating a second transformed code number, storage means in said one of said communication units for storing said second transformed code number, a data encrypting circuit located in said one of said communication units, said data encrypting circuit being responsive to said stored transformed code number and to said other source number received from said other communication

unit for encrypting said other source number received from said other communication unit using said stored second transformed code number as a key code to generate a second encrypted source number, and

means responsive to said encrypted source number and said second encrypted source number for authenticating said key loader when said encrypted source number and said second encrypted source number are equal.

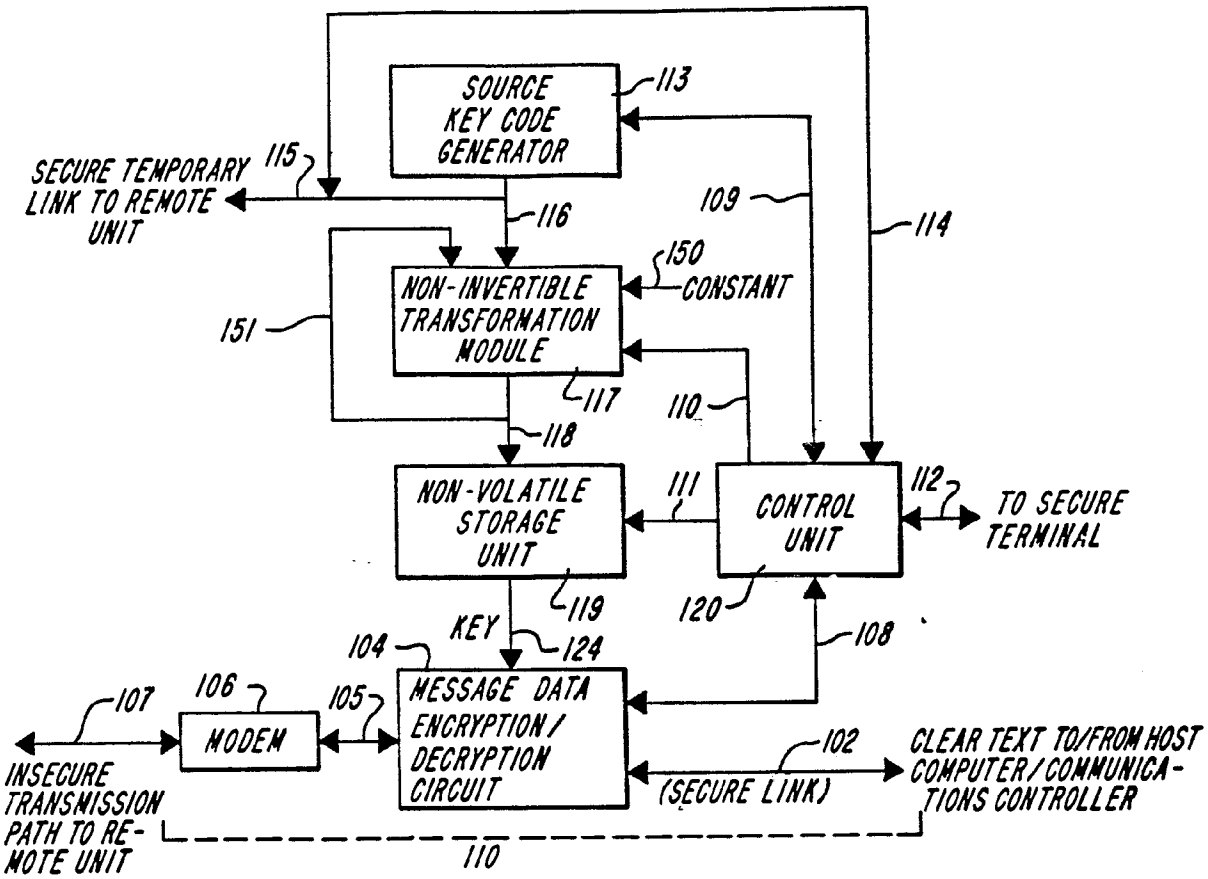
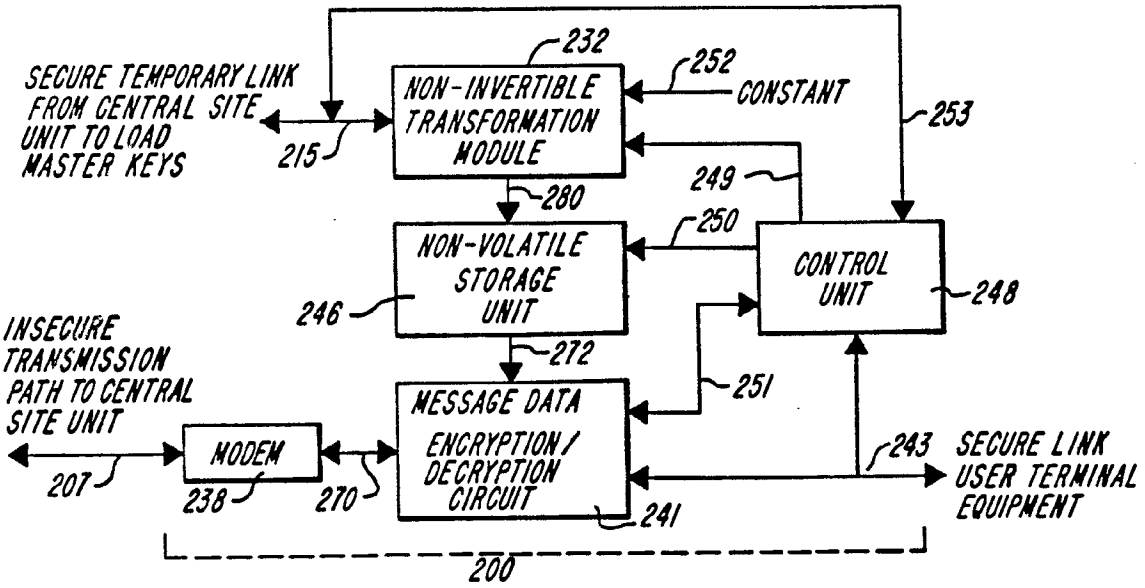

SOURCE KEY CODE GENERATOR
113
SECURE TEMPORARY LINK TO REMOTE UNIT
115
116
109
114
NON-INVERTIBLE TRANSFORMATION MODULE
150
CONSTANT
151
117
110
118
NON-VOLATILE STORAGE UNIT
111
CONTROL UNIT
112
TO SECURE TERMINAL
119
120
KEY
124
104
108
MESSAGE DATA ENCRYPTION/ DECRYPTION CIRCUIT
107
106
105
MODEM
INSECURE TRANSMISSION PATH TO REMOTE UNIT
102
(SECURE LINK)
CLEAR TEXT TO/FROM HOST COMPUTER/COMMUNICATIONS CONTROLLER
110

FIG. 1

FIG. 2


SECURE TEMPORARY LINK FROM CENTRAL SITE UNIT TO LOAD MASTER KEYS
215
232
NON-INVERTIBLE TRANSFORMATION MODULE
252
CONSTANT
253
249
280
NON-VOLATILE STORAGE UNIT
246
250
CONTROL UNIT
248
272
INSECURE TRANSMISSION PATH TO CENTRAL SITE UNIT
MESSAGE DATA ENCRYPTION/ DECRYPTION CIRCUIT
251
MODEM
207
238
270
241
243
SECURE LINK USER TERMINAL EQUIPMENT
200

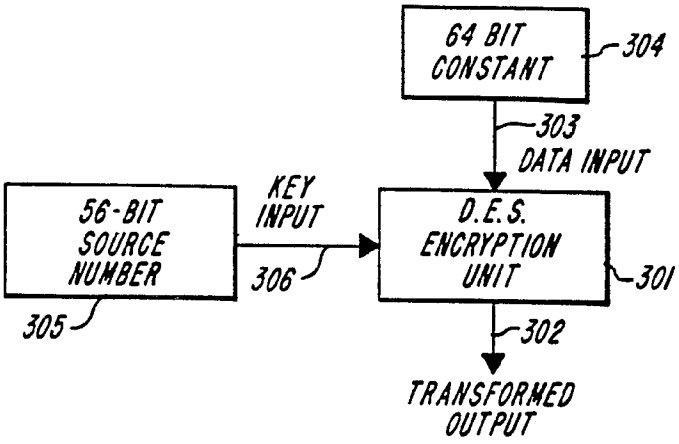

64 BIT CONSTANT
304
303
DATA INPUT
56-BIT SOURCE NUMBER
KEY INPUT
306
D.E.S. ENCRYPTION UNIT
301
305
302
TRANSFORMED OUTPUT

FIG. 3

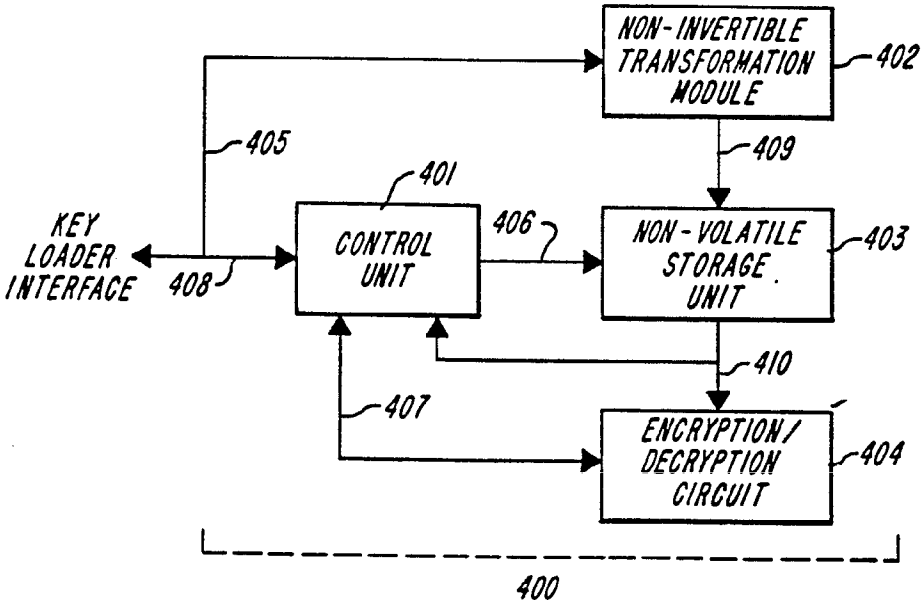

NON-INVERTIBLE TRANSFORMATION MODULE
402
405
409
401
KEY LOADER INTERFACE
408
CONTROL UNIT
406
NON-VOLATILE STORAGE UNIT
403
410
407
ENCRYPTION/ DECRYPTION CIRCUIT
404
400

FIG. 4

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 86/02644

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC[4]: H 04 L 9/00

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC[4]	H 04 L; H 04 K; G 06 F

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
A	Communications of the Association for Computing Machinery, volume 17, no. 1, August 1974, (New York, US), A. Evans, Jr. et al.: "A user authentication scheme not requiring secrecy in the computer", pages 437-442 see the whole document	1,3,6-8, 12-14,18, 21,29
A	EP, A, 0023074 (MOTOROLA) 28 January 1981 see claims 6-10; page 6, line 3 - page 9, line 20; page 25, line 17 - page 31, line 8	1,2,4,6,9, 12,15,18, 21,24,29, 31
A	DE, A, 3340582 (ANT) 23 May 1985 see the whole document	24,29,31
A	DE, A, 3244538 (ANT) 7 June 1984 see the whole document	24,29,31

./.

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
26th June 1987	27 JUL 1987
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	M. VAN MOL

Form PCT/ISA/210 (second sheet) (January 1985)

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category *	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No
A	EP, A, 0142013 (MARTE) 22 May 1985 see abstract, page 13, lines 29-32	5,10,11, 16,17,24

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON

INTERNATIONAL APPLICATION NO. PCT/US 86/02644 (SA 16964)

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 09/07/87

The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A- 0023074	28/01/81	JP-A-	55156444	05/12/80
		US-A-	4281216	28/07/81
DE-A- 3340582	23/05/85	NL-A-	8403416	03/06/85
DE-A- 3244538	07/06/84	NL-A-	8304120	02/07/84
EP-A- 0142013	22/05/85	None		